CHALMERS
UNIVERSITY OF TECHNOLOGY

Asymmetry Helps: Improved Private Information Retrieval Protocols for Distributed Storage

Asymmetry Helps: Improved Private Information Retrieval Protocols for Distributed Storage

Hsuan-Yin Lin[†], Siddhartha Kumar[†], Eirik Rosnes[†], and Alexandre Graell i Amat[‡]
[†]Simula UiB, N–5020 Bergen, Norway
[‡]Department of Electrical Engineering, Chalmers University of Technology, SE–41296 Gothenburg, Sweden

***Abstract*—We consider private information retrieval (PIR) for distributed storage systems (DSSs) with noncolluding nodes where data is stored using a non maximum distance separable (MDS) linear code. It was recently shown that if data is stored using a particular class of non-MDS linear codes, the *MDS-PIR capacity*, i.e., the maximum possible PIR rate for MDS-coded DSSs, can be achieved. For this class of codes, we prove that the PIR capacity is indeed equal to the MDS-PIR capacity, giving the first family of non-MDS codes for which the PIR capacity is known. For other codes, we provide asymmetric PIR protocols that achieve a strictly larger PIR rate compared to existing symmetric PIR protocols.**

I. Introduction

The concept of private information retrieval (PIR) was first introduced by Chor *et al.* [1]. A PIR protocol allows a user to privately retrieve an arbitrary data item stored in multiple servers (referred to as nodes in the sequel) without disclosing any information of which item is requested to the nodes. The efficiency of a PIR protocol is measured in terms of the total communication cost between the user and the nodes, which is equal to the sum of the upload and download costs. In distributed storage systems (DSSs), data is encoded by an $[n, k]$ linear code and then stored on n nodes in a distributed manner. Such DSSs are referred to as coded DSSs [2], [3].

One of the primary aims in PIR is the design of efficient PIR protocols from an information-theoretic perspective. Since the upload cost does not scale with the file size, the download cost dominates the total communication cost [3], [4]. Thus, the efficiency of a PIR protocol is commonly measured by the amount of information retrieved per downloaded symbol, referred to as the PIR rate. Sun and Jafar derived the maximum achievable PIR rate, the so-called *PIR capacity*, for the case of DSSs with replicated data [5], [6]. In the case where the data stored is encoded by an MDS storage code (the so-called *MDS-coded DSS*) and no nodes collude, a closed-form expression for the PIR capacity, referred to as the *MDS-PIR capacity*, was derived in [7].

In the earlier work [8]–[10], the authors focused on the properties of non-MDS storage codes in order to achieve the MDS-PIR capacity. In particular, in [9], [10] it was shown that the MDS-PIR capacity can be achieved for a special class of non-MDS linear codes, which, with some abuse of language, we refer to as *MDS-PIR capacity-achieving* codes (there might exist other codes outside of this class that achieve the MDS-PIR capacity). However, it is still unknown whether the MDS-PIR capacity is the best possible PIR rate that can be achieved for an arbitrarily coded DSS. In particular, an expression for the PIR capacity for coded DSSs with arbitrary linear storage codes is still missing.

In this paper, we consider the noncolluding case and first prove that the PIR capacity of coded DSSs that use the class of MDS-PIR capacity-achieving codes introduced in [9] is equal to the MDS-PIR capacity. We then address the fundamental question of what is the maximum achievable PIR rate for an arbitrarily coded DSS. To this purpose, we mainly consider non-MDS-PIR capacity-achieving codes. Most of the earlier works focus on designing symmetric PIR protocols and it was shown in [5], [7], [11] that any PIR scheme can be made symmetric for MDS-coded DSSs. However, this is in general not the case for non-MDS codes. Specifically, we propose an *asymmetric* PIR protocol, Protocol A, that allows asymmetry in the responses from the storage nodes. For non-MDS-PIR capacity-achieving codes, Protocol A achieves improved PIR rates compared to the PIR rates of existing symmetric PIR protocols. Furthermore, we present an asymmetric PIR protocol, Protocol B, that applies to non-MDS-PIR capacity-achieving codes that can be written as a direct sum of MDS-PIR capacity-achieving codes. Finally, we give an example showing that it is possible to construct an improved (compared to Protocol A) asymmetric PIR protocol. The protocol is code-dependent and strongly relies on finding *good* punctured MDS-PIR capacity-achieving subcodes of the non-MDS-PIR capacity-achieving code.

II. Preliminaries and System Model

A. Notation and Definitions

We denote by $\mathbb{N}$ the set of all positive integers and define $\mathbb{N}_a \triangleq \{1, 2, \ldots, a\}$. Vectors are denoted by lower case bold letters, matrices by upper case bold letters, and sets by calligraphic upper case letters, e.g., $\boldsymbol{x}$, $\boldsymbol{X}$, and $\mathcal{X}$ denote a vector, a matrix, and a set, respectively. In addition, $\mathcal{X}^{\mathrm{c}}$ denotes the complement of a set $\mathcal{X}$ in a universe set. The fonts of random and deterministic quantities are not distinguished typographically since it should be clear from the context. We denote a submatrix of $\boldsymbol{X}$ that is restricted in columns by the set $\mathcal{I}$ by $\boldsymbol{X}|_{\mathcal{I}}$. The function $\mathsf{LCM}(n_1, n_2, \ldots, n_a)$ computes the lowest common multiple of a positive integers $n_1, n_2, \ldots, n_a$. The function $\mathsf{H}(\cdot)$ represents the entropy of its argument and

This work was partially funded by the Research Council of Norway (grant 240985/F20) and the Swedish Research Council (grant #2016-04253).

$\mathsf{I}(\cdot;\cdot)$ denotes the mutual information of the first argument with respect to the second argument. $(\cdot)^\intercal$ denotes the transpose of its argument. We use the customary code parameters $[n,k]$ to denote a code $\mathcal{C}$ over the finite field GF(q) of blocklength n and dimension k. A generator matrix of $\mathcal{C}$ is denoted by $\boldsymbol{G}^{\mathcal{C}}$, while $\mathcal{C}^{\boldsymbol{G}}$ represents the corresponding code generated by $\boldsymbol{G}$. The function $\chi(\boldsymbol{x})$ denotes the support of a vector $\boldsymbol{x}$, while the support of a code $\mathcal{C}$ is defined as the set of coordinates where not all codewords are zero. A set of coordinates of $\mathcal{C}$, $\mathcal{I} \subseteq \mathbb{N}_n$, of size k is said to be an *information set* if and only if $\boldsymbol{G}^{\mathcal{C}}|_{\mathcal{I}}$ is invertible. The s-th generalized Hamming weight of an $[n,k]$ code $\mathcal{C}$, denoted by $d_s^{\mathcal{C}}$, $s \in \mathbb{N}_k$, is defined as the cardinality of the smallest support of an s-dimensional subcode of $\mathcal{C}$.

B. System Model

We consider a DSS that stores f files $\boldsymbol{X}^{(1)}, \ldots, \boldsymbol{X}^{(f)}$, where each file $\boldsymbol{X}^{(m)} = (x_{i,l}^{(m)})$, $m \in \mathbb{N}_f$, can be seen as a $\beta \times k$ matrix over GF(q) with $\beta, k \in \mathbb{N}$. Each file is encoded using a linear code as follows. Let $\boldsymbol{x}_i^{(m)} = \big(x_{i,1}^{(m)}, \ldots, x_{i,k}^{(m)}\big)$, $i \in \mathbb{N}_\beta$, be a message vector corresponding to the i-th row of $\boldsymbol{X}^{(m)}$. Each $\boldsymbol{x}_i^{(m)}$ is encoded by an $[n,k]$ code $\mathcal{C}$ over GF(q) into a length-n codeword $\boldsymbol{c}_i^{(m)} = \big(c_{i,1}^{(m)}, \ldots, c_{i,n}^{(m)}\big)$. The βf generated codewords $\boldsymbol{c}_i^{(m)}$ are then arranged in the array $\boldsymbol{C} = \big((\boldsymbol{C}^{(1)})^\intercal | \ldots | (\boldsymbol{C}^{(f)})^\intercal\big)^\intercal$ of dimensions $\beta f \times n$, where $\boldsymbol{C}^{(m)} = \big((\boldsymbol{c}_1^{(m)})^\intercal | \ldots | (\boldsymbol{c}_\beta^{(m)})^\intercal\big)^\intercal$. The code symbols $c_{1,l}^{(m)}, \ldots, c_{\beta,l}^{(m)}$, $m \in \mathbb{N}_f$, for all f files are stored on the l-th storage node, $l \in \mathbb{N}_n$.

C. Privacy Model

To retrieve file $\boldsymbol{X}^{(m)}$ from the DSS, the user sends a random query $Q_l^{(m)}$ to the l-th node for all $l \in \mathbb{N}_n$. In response to the received query, node l sends the response $A_l^{(m)}$ back to the user. $A_l^{(m)}$ is a deterministic function of $Q_l^{(m)}$ and the code symbols stored in the node.

Definition 1: Consider a DSS with n noncolluding nodes storing f files. A user who wishes to retrieve the m-th file sends the queries $Q_l^{(m)}$, $l \in \mathbb{N}_n$, to the storage nodes, which return the responses $A_l^{(m)}$. This scheme achieves perfect information-theoretic PIR if and only if

Privacy:

$$\mathsf{I}\big(m; Q_l^{(m)}, A_l^{(m)}, \boldsymbol{X}^{(1)}, \ldots, \boldsymbol{X}^{(f)}\big) = 0, \, \forall\, l \in \mathbb{N}_n, \quad \text{(1a)}$$

Recovery:

$$\mathsf{H}\big(\boldsymbol{X}^{(m)} \,\big|\, A_1^{(m)}, \ldots, A_n^{(m)}, Q_1^{(m)}, \ldots, Q_n^{(m)}\big) = 0. \quad \text{(1b)}$$

D. PIR Rate and Capacity

Definition 2: The PIR rate of a PIR protocol, denoted by R, is the amount of information retrieved per downloaded symbol, i.e., $\mathsf{R} \triangleq \frac{\beta k}{\mathsf{D}}$, where D is the total number of downloaded symbols for the retrieval of a single file.

We will write $\mathsf{R}(\mathcal{C})$ to highlight that the PIR rate depends on the underlying storage code $\mathcal{C}$. It was shown in [7] that for the noncolluding case and for a given number of files f stored using an $[n,k]$ MDS code, the MDS-PIR capacity is

$$\mathsf{C}_f^{[n,k]} \triangleq \frac{n-k}{n}\left[1 - \left(\frac{k}{n}\right)^f\right]^{-1}, \quad (2)$$

where superscript "$[n,k]$" indicates the code parameters of the underlying MDS storage code. When the number of files f tends to infinity, (2) reduces to $\mathsf{C}_\infty^{[n,k]} \triangleq \lim_{f\to\infty} \mathsf{C}_f^{[n,k]} = \frac{n-k}{n}$, which we refer to as the asymptotic MDS-PIR capacity. Note that for the case of non-MDS linear codes, the PIR capacity is unknown.

E. MDS-PIR Capacity-Achieving Codes

In [9], two symmetric PIR protocols for coded DSSs, named Protocol 1 and Protocol 2, were proposed. Their PIR rates depend on the following property of the underlying storage code $\mathcal{C}$.

Definition 3: Let $\mathcal{C}$ be an arbitrary $[n,k]$ code. A $\nu \times n$ binary matrix $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ is said to be a *PIR achievable rate matrix* for $\mathcal{C}$ if the following conditions are satisfied.

1) The Hamming weight of each column of $\boldsymbol{\Lambda}_{\kappa,\nu}$ is κ, and
2) for each matrix row $\boldsymbol{\lambda}_i$, $i \in \mathbb{N}_\nu$, $\chi(\boldsymbol{\lambda}_i)$ always contains an information set.

The following theorem gives the achievable PIR rate of Protocol 1 from [9, Thm. 1].

Theorem 1: Consider a DSS that uses an $[n,k]$ code $\mathcal{C}$ to store f files. If a PIR achievable rate matrix $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ exists, then the PIR rate

$$\mathsf{R}_{f,\mathsf{S}}(\mathcal{C}) \triangleq \frac{(\nu-\kappa)k}{\kappa n}\left[1 - \left(\frac{\kappa}{\nu}\right)^f\right]^{-1} \quad (3)$$

is achievable.

In (3), we use subscript S to indicate that this PIR rate is achievable by the symmetric Protocol 1 in [9]. Define $\mathsf{R}_{\infty,\mathsf{S}}(\mathcal{C})$ as the limit of $\mathsf{R}_{f,\mathsf{S}}(\mathcal{C})$ as the number of files f tends to infinity, i.e., $\mathsf{R}_{\infty,\mathsf{S}}(\mathcal{C}) \triangleq \lim_{f\to\infty} \mathsf{R}_{f,\mathsf{S}}(\mathcal{C}) = \frac{(\nu-\kappa)k}{\kappa n}$. The asymptotic PIR rate $\mathsf{R}_{\infty,\mathsf{S}}(\mathcal{C})$ is also achieved by the file-independent Protocol 2 from [9].

Corollary 1: If a PIR achievable rate matrix $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ with $\frac{\kappa}{\nu} = \frac{k}{n}$ exists for an $[n,k]$ code $\mathcal{C}$, then the MDS-PIR capacity in (2) is achievable.

Definition 4: A PIR achievable rate matrix $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ with $\frac{\kappa}{\nu} = \frac{k}{n}$ for an $[n,k]$ code $\mathcal{C}$ is called an *MDS-PIR capacity-achieving* matrix, and $\mathcal{C}$ is referred to as an *MDS-PIR capacity-achieving* code.

The following theorem from [9, Thm. 3] provides a necessary condition for the existence of an MDS-PIR capacity-achieving matrix.

Theorem 2: If an MDS-PIR capacity-achieving matrix exists for an $[n,k]$ code $\mathcal{C}$, then $d_s^{\mathcal{C}} \geq \frac{n}{k}s$, $\forall\, s \in \mathbb{N}_k$.

III. PIR Capacity for MDS-PIR Capacity-Achieving Codes

In this section, we prove that the PIR capacity of MDS-PIR capacity-achieving codes is equal to the MDS-PIR capacity.

TABLE I
PROTOCOL 1 WITH A $[5,3]$ NON-MDS-PIR CAPACITY-ACHIEVING CODE FOR $f=2$

		Node 1	Node 2	Node 3	Node 4	Node 5
repetition 1	round 1	$y^{(1)}_{2(2-1)+1,1}$ $y^{(1)}_{2(2-1)+2,1}$	$y^{(1)}_{2(1-1)+1,2}$ $y^{(1)}_{2(1-1)+2,2}$	$y^{(1)}_{2(1-1)+1,3}$ $y^{(1)}_{2(1-1)+2,3}$	$y^{(1)}_{2(1-1)+1,4}$ $y^{(1)}_{2(1-1)+2,4}$	$y^{(1)}_{2(1-1)+1,5}$ $y^{(1)}_{2(1-1)+2,5}$
		$y^{(2)}_{3\cdot 0+2,1}$ $y^{(2)}_{3\cdot 0+3,1}$	$y^{(2)}_{3\cdot 0+1,2}$ $y^{(2)}_{3\cdot 0+3,2}$	$y^{(2)}_{5\cdot 0+1,3}$ $y^{(2)}_{3\cdot 0+3,3}$	$y^{(2)}_{3\cdot 0+1,4}$ $y^{(2)}_{3\cdot 0+2,4}$	$y^{(2)}_{3\cdot 0+1,5}$ $y^{(2)}_{3\cdot 0+2,5}$
	rnd. 2	$y^{(1)}_{2\cdot 3+2,1}+y^{(2)}_{3\cdot 0+1,1}$	$y^{(1)}_{2\cdot 3+1,2}+y^{(2)}_{3\cdot 0+2,2}$	$y^{(1)}_{2\cdot 3+1,3}+y^{(2)}_{3\cdot 0+2,3}$	$y^{(1)}_{2\cdot 3+1,4}+y^{(2)}_{3\cdot 0+3,4}$	$y^{(1)}_{2\cdot 3+1,5}+y^{(2)}_{3\cdot 0+3,5}$
repetition 2	round 1	$y^{(1)}_{2(3-1)+1,1}$ $y^{(1)}_{2(3-1)+2,1}$	$y^{(1)}_{2(3-1)+1,2}$ $y^{(1)}_{2(3-1)+2,2}$	$y^{(1)}_{2(3-1)+1,3}$ $y^{(1)}_{2(3-1)+2,3}$	$y^{(1)}_{2(2-1)+1,4}$ $y^{(1)}_{2(2-1)+2,4}$	$y^{(1)}_{2(2-1)+1,5}$ $y^{(1)}_{2(2-1)+2,5}$
		$y^{(2)}_{3\cdot 1+2,1}$ $y^{(2)}_{3\cdot 1+3,1}$	$y^{(2)}_{3\cdot 1+1,2}$ $y^{(2)}_{3\cdot 1+3,2}$	$y^{(2)}_{3\cdot 1+1,3}$ $y^{(2)}_{3\cdot 1+3,3}$	$y^{(2)}_{3\cdot 1+1,4}$ $y^{(2)}_{3\cdot 1+2,4}$	$y^{(2)}_{3\cdot 1+1,5}$ $y^{(2)}_{3\cdot 1+2,5}$
	rnd. 2	$y^{(1)}_{2\cdot 3+3,1}+y^{(2)}_{3\cdot 1+1,1}$	$y^{(1)}_{2\cdot 3+3,2}+y^{(2)}_{3\cdot 1+2,2}$	$y^{(1)}_{2\cdot 3+3,3}+y^{(2)}_{3\cdot 1+2,3}$	$y^{(1)}_{2\cdot 3+2,4}+y^{(2)}_{3\cdot 1+3,4}$	$y^{(1)}_{2\cdot 3+2,5}+y^{(2)}_{3\cdot 1+3,5}$

Theorem 3: Consider a DSS that uses an $[n,k]$ MDS-PIR capacity-achieving code $\mathcal{C}$ to store f files. Then, the maximum achievable PIR rate over all possible PIR protocols, i.e., the PIR capacity, is equal to the MDS-PIR capacity $\mathsf{C}_f^{[n,k]}$ in (2).

Proof: See [12, App. A]. ∎

Theorem 3 provides an expression for the PIR capacity for the family of MDS-PIR capacity-achieving codes (i.e., (2)). Moreover, for any finite number of files f and in the asymptotic case where f tends to infinity, the PIR capacity can be achieved using Protocols 1 and 2 from [9], respectively.

IV. ASYMMETRY HELPS: IMPROVED PIR PROTOCOLS

In this section, we present three asymmetric PIR protocols for non-MDS-PIR capacity-achieving codes, illustrating that asymmetry helps to improve the PIR rate. By asymmetry we mean that the number of symbols downloaded from the different nodes is not the same, i.e., for any fixed $m \in \mathbb{N}_f$, the entropies $\mathsf{H}(A_l^{(m)})$, $l \in \mathbb{N}_n$, may be different. This is in contrast to the case of MDS codes, where any asymmetric protocol can be made symmetric while preserving its PIR rate [5], [7], [11]. We start with a simple motivating example showing that the PIR rate of Protocol 1 from [9] can be improved for some underlying storage codes.

A. Protocol 1 From [9] is Not Optimal in General

Example 1: Consider the $[5,3]$ code $\mathcal{C}$ with generator matrix

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

The smallest possible value of $\frac{\kappa}{\nu}$ for which a PIR achievable rate matrix exists is $\frac{2}{3}$ and a corresponding PIR achievable rate matrix is

$$\boldsymbol{\Lambda}_{2,3} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

It is easy to verify that $\boldsymbol{\Lambda}_{2,3}$ above is a PIR achievable rate matrix for code $\mathcal{C}$. Thus, the largest PIR rate for $f=2$ files with Protocol 1 from [9] is $\mathsf{R}_{2,\mathsf{S}} = \frac{3^3}{5\cdot 10} = \frac{27}{50}$. In Table I (taken from [9, Sec. IV]), we list the downloaded sums of code symbols when retrieving file $\boldsymbol{X}^{(1)}$ and $f=2$ files are stored. In the table, for each $m \in \mathbb{N}_2$ and $\beta = \nu^f = 3^2$, the interleaved code array $\boldsymbol{Y}^{(m)}$ with row vectors $\boldsymbol{y}_i^{(m)} = \boldsymbol{c}_{\pi(i)}^{(m)}$, $i \in \mathbb{N}_{3^2}$, is generated (according to Protocol 1 from [9]) by a randomly selected permutation function $\pi(\cdot)$.

Observe that since $\{2,3,4\} \subset \chi(\boldsymbol{\lambda_1}) = \{2,3,4,5\}$ is an information set of $\mathcal{C}$, the five sums of

$$\{y^{(1)}_{2(1-1)+1,5}, y^{(1)}_{2(1-1)+2,5}, y^{(2)}_{3\cdot 0+1,5}, y^{(1)}_{2\cdot 3+1,5}+y^{(2)}_{3\cdot 0+3,5}, y^{(2)}_{3\cdot 1+1,5}\}$$

are not necessarily required to recover $\boldsymbol{X}^{(1)}$. For privacy concerns, notice that the remaining sums of code symbols from the 5-th node would be

$$\{y^{(2)}_{3\cdot 0+2,5}, y^{(1)}_{2(2-1)+1,5}, y^{(1)}_{2\cdot(2-1)+2,5}, y^{(2)}_{3\cdot 1+2,5}, y^{(1)}_{2\cdot 3+2,5}+y^{(2)}_{3\cdot 1+3,5}\}.$$

This ensures the privacy condition, since for every combination of files, the user downloads the same number of linear sums. This shows that by allowing asymmetry in the responses from the storage nodes, the PIR rate can be improved to $\frac{27}{50-5} = \frac{27}{45} = \frac{3}{5}$, which is much closer to the MDS-PIR capacity $\mathsf{C}_2^{[5,3]} = \frac{1}{1+\frac{3}{5}} = \frac{5}{8}$.

Example 1 indicates that for a coded DSS using a non-MDS-PIR capacity-achieving code, there may exist an asymmetric PIR scheme that improves the PIR rate of the symmetric Protocol 1 from [9].

B. Protocol A: A General Asymmetric PIR Protocol

In this subsection, we show that for non-MDS-PIR capacity-achieving codes, by discarding the redundant coordinates that are not required to form an information set within $\chi(\boldsymbol{\lambda}_i)$, $i \in \mathbb{N}_\nu$, it is always possible to obtain a larger PIR rate compared to that of Protocol 1 from [9].

Theorem 4: Consider a DSS that uses an $[n,k]$ code $\mathcal{C}$ to store f files. If a PIR achievable rate matrix $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ exists, then the PIR rate

$$\mathsf{R}_{f,\,\mathsf{A}}(\mathcal{C}) \triangleq \left(1-\frac{\kappa}{\nu}\right)\left[1-\left(\frac{\kappa}{\nu}\right)^f\right]^{-1} \tag{4}$$

is achievable.

Proof: See [12, App. B]. ∎

Proposition 1 below can be easily verified using [9, Lem. 2].

Proposition 1: Consider a DSS that uses an $[n,k]$ code $\mathcal{C}$ to store f files. Then, $\mathsf{R}_{f,\mathsf{S}}(\mathcal{C}) \leq \mathsf{R}_{f,\mathsf{A}}(\mathcal{C}) \leq \mathsf{C}_f^{[n,k]}$ with equality if and only if $\mathcal{C}$ is an MDS-PIR capacity-achieving code.

In the following, we refer to the asymmetric PIR protocol that achieves the PIR rate in Theorem 4 as Protocol A (thus the subscript A in $\mathsf{R}_{f,\mathsf{A}}(\mathcal{C})$ in (4)). Similar to Theorem 1, there also exists an asymmetric file-independent PIR protocol that achieves the asymptotic PIR rate $\mathsf{R}_{\infty,\mathsf{A}}(\mathcal{C}) \triangleq \lim_{f\to\infty} \mathsf{R}_{f,\mathsf{A}}(\mathcal{C}) = 1-\frac{\kappa}{\nu}$ and we simply refer to this protocol as the file-independent Protocol A.[1]

C. Protocol B: An Asymmetric PIR Protocol for a Special Class of Non-MDS-PIR Capacity-Achieving Codes

In this subsection, we focus on designing an asymmetric PIR protocol, referred to as Protocol B, for a special class of $[n,k]$ non-MDS-PIR capacity-achieving codes, where the code is isometric to a *direct sum* of $P \in \mathbb{N}_n$ MDS-PIR capacity-achieving codes [13, Ch. 2]. Without loss of generality, we assume that the generator matrix $\boldsymbol{G}$ of an $[n,k]$ non-MDS-PIR capacity-achieving code $\mathcal{C}$ has the structure

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{G}_1 & & & \\ & \boldsymbol{G}_2 & & \\ & & \ddots & \\ & & & \boldsymbol{G}_P \end{pmatrix}, \tag{5}$$

where $\boldsymbol{G}_p$, of size $k_p \times n_p$, is the generator matrix of a punctured MDS-PIR capacity-achieving subcode $\mathcal{C}^{\boldsymbol{G}_p}$, $p \in \mathbb{N}_P$.

Theorem 5: Consider a DSS that uses an $[n,k]$ non-MDS-PIR capacity-achieving code $\mathcal{C}$ to store f files. If the code $\mathcal{C}$ is isometric to a direct sum of $P \in \mathbb{N}_n$ MDS-PIR capacity-achieving codes as in (5), then the PIR rate

$$\mathsf{R}_{f,\mathsf{B}}(\mathcal{C}) \triangleq \left(\sum_{p=1}^{P} \frac{k_p}{k} \left(\mathsf{C}_f^{[n_p,k_p]} \right)^{-1} \right)^{-1}$$

is achievable. Moreover, the asymptotic PIR rate

$$\mathsf{R}_{\infty,\mathsf{B}}(\mathcal{C}) \triangleq \lim_{f\to\infty} \mathsf{R}_{f,\mathsf{B}}(\mathcal{C}) = \left(\sum_{p=1}^{P} \frac{k_p}{k} \left(\mathsf{C}_\infty^{[n_p,k_p]} \right)^{-1} \right)^{-1}$$

is achievable by a file-independent PIR protocol.

Proof: See [12, App. C]. ∎

We remark that Protocol B requires $\beta = \mathsf{LCM}(\beta_1, \ldots, \beta_P)$ stripes, where β_p, $p \in \mathbb{N}_P$, is the smallest number of stripes of either Protocol 1 or Protocol 2 for a DSS that uses only the punctured MDS-PIR capacity-achieving subcode $\mathcal{C}^{\boldsymbol{G}_p}$ to store f files [12, App. C].

Theorem 5 can be used to obtain a larger PIR rate for the non-MDS-PIR capacity-achieving code in Example 1.

Example 2: Continuing with Example 1, by elementary matrix operations, the generator matrix of the $[5,3]$ code of Example 1 is equivalent to the generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \boldsymbol{G}_1 & \\ & \boldsymbol{G}_2 \end{pmatrix}.$$

It can easily be verified that both $\mathcal{C}^{\boldsymbol{G}_1}$ and $\mathcal{C}^{\boldsymbol{G}_2}$ are MDS-PIR capacity-achieving codes. Hence, from Theorem 5, the asymptotic PIR rate $\mathsf{R}_{\infty,\mathsf{B}} = \left(\frac{2}{3}\frac{1}{1-\frac{2}{3}} + \frac{1}{3}\frac{1}{1-\frac{1}{2}} \right)^{-1} = \frac{3}{8}$ is achievable. The rate $\mathsf{R}_{\infty,\mathsf{B}} = \frac{3}{8}$ is strictly larger than both $\mathsf{R}_{\infty,\mathsf{S}} = \frac{3}{10}$ and $\mathsf{R}_{\infty,\mathsf{A}} = \frac{1}{3}$.

D. Protocol C: Code-Dependent Asymmetric PIR Protocol

In this subsection, we provide a code-dependent, but file-independent asymmetric PIR protocol for non-MDS-PIR capacity-achieving codes that cannot be decomposed into a direct sum of MDS-PIR capacity-achieving codes as in (5). The protocol is tailor-made for each class of storage codes. The main principle of the protocol is to further reduce the number of downloaded symbols by looking at punctured MDS-PIR capacity-achieving subcodes. Compared to Protocol A, which is simpler and allows for a closed-form expression for its PIR rate, Protocol C gives larger PIR rates.

The file-independent Protocol 2 from [9] utilizes *interference symbols*. An interference symbol can be defined through a summation as [9]

$$I_{(h-1)k+h'} \triangleq \sum_{m=1}^{f} \sum_{j=(m-1)\beta+1}^{m\beta} u_{h,j} x_{j-(m-1)\beta,h'}^{(m)},$$

where $h, h' \in \mathbb{N}_k$ and the symbols $u_{h,j}$ are chosen independently and uniformly at random from the same field as the code symbols.

Example 3: Consider a $[9,5]$ code $\mathcal{C}$ with generator matrix

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

It has $d_2^{\mathcal{C}} = 3 < \frac{9}{5} \cdot 2$, thus it is not MDS-PIR capacity-achieving (see Theorem 2). Note that this code cannot be decomposed into a direct sum of MDS-PIR capacity-achieving codes as in (5).

The smallest $\frac{\kappa}{\nu}$ for which a PIR achievable rate matrix exists for this code is $\frac{2}{3}$, and a corresponding PIR achievable rate matrix is

$$\boldsymbol{\Lambda}_{2,3} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The idea of the file-independent Protocol 2 from [9] is to use the information sets $\mathcal{I}_1 = \{2,6,7,8,9\}$ and $\mathcal{I}_2 = \{1,3,4,5,9\}$ to recover the $\beta k = 1 \cdot 5$ requested file symbols that are located in $\mathcal{I}_3 = \{1,2,3,4,5\}$. Specifically, we use the information set $\mathcal{I}_1$ to reconstruct the required code symbols located in $\chi(\boldsymbol{\lambda}_1)^{\mathrm{c}} = \{1,3,4,5\}$ and $\mathcal{I}_2 \subseteq \chi(\boldsymbol{\lambda}_2) = \{1,3,4,5,6,7,8,9\}$ to reconstruct the required code symbol located in $\chi(\boldsymbol{\lambda}_2)^{\mathrm{c}} = \{2\}$. Since the code coordinates

[1] As for Protocol 1 and Protocol 2 from [9, Remark 2], $\boldsymbol{\Lambda}_{\kappa,\nu}(\mathcal{C})$ can be used for both Protocol A and the file-independent Protocol A.

TABLE II
RESPONSES BY PROTOCOL C WITH A $[9,5]$ NON-MDS-PIR CAPACITY-ACHIEVING CODE

Subresponses	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9
Subresponse 1	$I_1 + x_{1,1}^{(m)}$	I_2	$I_3 + x_{1,3}^{(m)}$	$I_4 + x_{1,4}^{(m)}$	$I_5 + x_{1,5}^{(m)}$	$I_4 + I_5$	$I_3 + I_5$	$I_3 + I_4 + I_5$	$I_1 + I_2 + I_4 + I_5$
Subresponse 2	I_6	$I_7 + x_{1,2}^{(m)}$		I_9	I_{10}				$I_6 + I_7 + I_9 + I_{10}$

TABLE III
PIR RATE FOR DIFFERENT CODES AND PROTOCOLS

Code	$\frac{\kappa}{\nu}$	$\mathsf{R}_{\infty,\mathsf{S}}$	$\mathsf{R}_{\infty,\mathsf{A}}$	$\mathsf{R}_{\infty,\mathsf{B}}$	$\mathsf{R}_{\infty,\mathsf{C}}$	$\mathsf{C}_{\infty}^{[n,k]}$
$\mathcal{C}_1 : [5,3]$	$2/3$	0.3	0.3333	0.375	0.375	0.4
$\mathcal{C}_2 : [9,5]$	$2/3$	0.2778	0.3333	–	0.3571	0.4444
$\mathcal{C}_3 : [7,4]$	$3/5$	0.3810	0.4	–	0.4	0.4286
$\mathcal{C}_4 : [11,6]$	$3/4$	0.1818	0.25	–	0.2824	0.4545

$\{1,2,4,5,9\}$ form an $[n',k'] = [5,4]$ punctured MDS-PIR capacity-achieving subcode $\mathcal{C}^{\boldsymbol{G}'}$ with generator matrix

$$\boldsymbol{G}' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

it can be seen that the code coordinates $\{1,4,5,9\}$ are sufficient to correct the erasure located in $\chi(\boldsymbol{\lambda}_2)^{\mathrm{c}}$. Therefore, compared to Protocol A, we can further reduce the required number of downloaded symbols. The responses from the nodes when retrieving file $\boldsymbol{X}^{(m)}$ are listed in Table II. The PIR rate of Protocol C is then equal to $\mathsf{R}_{\infty,\mathsf{C}} = \frac{1\cdot 5}{n+n'} = \frac{5}{14} < \frac{4}{9} = \mathsf{C}_{\infty}^{[9,5]}$, which is strictly larger than $\mathsf{R}_{\infty,\mathsf{A}} = \frac{1}{3}$. It can readily be seen from Table II that the privacy condition in (1a) is ensured.

Finally, we remark that, using the same principle as outlined above, other punctured MDS-PIR capacity-achieving subcodes can be used to construct a valid protocol, giving the same PIR rate. For instance, we could pick the two punctured subcodes $\mathcal{C}^{\boldsymbol{G}_1}$ and $\mathcal{C}^{\boldsymbol{G}_2}$ with generator matrices

$$\boldsymbol{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \boldsymbol{G}_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

respectively.

Example 3 above illustrates the main working principle of Protocol C and how the redundant set of code coordinates is taken into account. Its general description is given in [12]. However, some numerical results are given below, showing that it can attain larger PIR rates than Protocol A.

V. NUMERICAL RESULTS

In Table III, we compare the PIR rates for different protocols using several binary linear codes. The second column gives the smallest fraction $\frac{\kappa}{\nu}$ for which a PIR achievable rate matrix exists. In the table, code $\mathcal{C}_1$ is from Example 1, code $\mathcal{C}_2$ is from Example 3, $\mathcal{C}_3$ is a $[7,4]$ code with generator matrix $(1,2,4,8,8,14,5)$ (in decimal form, e.g., $(1,0,1,1)^{\mathsf{T}}$ is represented by 13) and $d_3^{\mathcal{C}_3} = 5 < \frac{7}{4}\cdot 3$, and $\mathcal{C}_4$ is an $[11,6]$ code with generator matrix $(1,2,4,8,16,32,48,40,24,56,55)$ and $d_3^{\mathcal{C}_4} = 4 < \frac{11}{6}\cdot 3$. Note that $\mathcal{C}_2$, $\mathcal{C}_3$, and $\mathcal{C}_4$ cannot be decomposed into a direct sum of MDS-PIR capacity-achieving codes as in (5). For all presented codes except $\mathcal{C}_3$, Protocol C achieves strictly larger PIR rate than Protocol A, although smaller than the MDS-PIR capacity.

VI. CONCLUSION

We proved that the PIR capacity for MDS-PIR capacity-achieving codes is equal to the MDS-PIR capacity for the case of noncolluding nodes, giving the first family of non-MDS codes for which the PIR capacity is known. We also showed that allowing asymmetry in the responses from the storage nodes yields larger PIR rates compared to symmetric protocols in the literature when the storage code is a non-MDS-PIR capacity-achieving code. We proposed three asymmetric protocols and compared them in terms of PIR rate for different storage codes.

REFERENCES

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in *Proc. 36th IEEE Symp. Found. Comp. Sci.*, Milwaukee, WI, USA, Oct. 23–25, 1995, pp. 41–50.

[2] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "One extra bit of download ensures perfectly private information retrieval," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun. 29 – Jul. 4, 2014, pp. 856–860.

[3] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private information retrieval for coded storage," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 14–19, 2015, pp. 2842–2846.

[4] R. Tajeddine and S. El Rouayheb, "Private information retrieval from MDS coded data in distributed storage systems," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 10–15, 2016, pp. 1411–1415.

[5] H. Sun and S. A. Jafar, "The capacity of private information retrieval," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4075–4088, Jul. 2017.

[6] ——, "The capacity of robust private information retrieval with colluding databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2361–2370, Apr. 2018.

[7] K. Banawan and S. Ulukus, "The capacity of private information retrieval from coded databases," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1945–1956, Mar. 2018.

[8] S. Kumar, E. Rosnes, and A. Graell i Amat, "Private information retrieval in distributed storage systems using an arbitrary linear code," in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 25–30, 2017, pp. 1421–1425.

[9] S. Kumar, H.-Y. Lin, E. Rosnes, and A. Graell i Amat, "Achieving maximum distance separable private information retrieval capacity with linear codes," Dec. 2017, arXiv:1712.03898v3 [cs.IT]. [Online]. Available: https://arxiv.org/abs/1712.03898

[10] H.-Y. Lin, S. Kumar, E. Rosnes, and A. Graell i Amat, "An MDS-PIR capacity-achieving protocol for distributed storage using non-MDS linear codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, Jun. 17–22, 2018, pp. 966–970.

[11] H. Sun and S. A. Jafar, "Private information retrieval from MDS coded data with colluding servers: Settling a conjecture by Freij-Hollanti et al." in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 25–30, 2017, pp. 1893–1897.

[12] H.-Y. Lin, S. Kumar, E. Rosnes, and A. Graell i Amat, "On the fundamental limit of private information retrieval for coded distributed storage," Aug. 2018, arXiv:1808.09018v2 [cs.IT]. [Online]. Available: https://arxiv.org/abs/1808.09018

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.